

Remarks/Arguments:

Claims 1-2, 4-26, and 28-32 remain in this application. Claims 1, and 10-25 were amended herein.

The Office Action rejected claims 1-32 (of which 1-2, 4-26, and 28-32 are pending) under 35 U.S.C. §101 as being directed to non-statutory subject matter. Applicant respectfully requests that this rejection of claims 1-2, 4-26, and 28-32 be withdrawn as the amendments previously entered were sufficient to overcome the rejection, and the amendments contained herein make it even clearer that the rejection should be withdrawn.

Applicant respectfully notes that the Interview Summary of the August 5, 2004 interview states: "Agreement was reached on proposed amendments to the claims to overcome the 101 rejections in the Office Action submitted on March 21, 2004 consisting, inter alia, defining a machine or computing device to perform the operations listed in the claims." Amendments consistent with the agreement reached were entered in the Applicant's response to the previous Office Action.

Support for the §101 rejection in the current Office Action is asserted by the Office Action to be found in the fact that the claimed invention is not supported by either a specific or substantial asserted utility or a well established utility. The Applicant respectfully disagrees in that: (a) the application as filed describes the utility of the claimed invention, (b) utility of apparatus that solve systems of linear equations is well known; and (c) there is no requirement that an apparatus claim recite an intended use.

Regardless, although not necessary to overcome the rejection, the Applicant has chosen to further amend claims 1 and 10-16, and 25 to recite use of the apparatus or method in one of: secret communications by encryption and decryption; digital signature and verification; and data conversion including encoding and decoding of data. Applicant also respectfully points out that claims 17-24 already recite an intended use that describes the utility of the claimed subject matter as they recites use of an inverse *I* to decrypt encrypted digital content recorded on a record medium in order to reproduce the record medium.

Support for the §101 rejection in the current Office Action is also asserted by the Office Action to be found in the fact that the claimed invention is directed to an apparatus comprising machine readable memory that provides instructions for solving a system of linear equations, and that the claimed function can be practiced mentally in conjunction with pen and paper and does not produce a useful, concrete and tangible result. Applicant respectfully requests that this assertion be reconsidered as the prior forms of the rejected claims included elements (such as a machine readable memory) that prevented pure mental use of the methods described from falling within the scope of the claims, and the prior form of the claims claimed methods and apparatus that produced useful, concrete and tangible result.

Regardless, although not necessary to overcome the rejection, the Applicant has chosen to amend claims 1, and 10-25 to include additional recitations that: (a) show use of the computed solution or inverse to perform one of: secret communication by encryption and decryption; digital signature generation and verification; and data conversion including encoding and decoding of data, by using the computed inverse I , or (b) include means for using I to decrypt the encrypted digital content recorded on the record medium.

In light of the foregoing, the Applicant respectfully requests that the §101 rejection of claims 1-2, 4-26, and 28-32 be withdrawn.

Claims 1-32 (of which 1-2, 4-26, and 28-32 are pending) were also rejected under 35 U.S.C. §112 as not clearly showing how to use the claimed invention. The Applicant respectfully traverses as (a) there is no requirement under §112 that claims, particularly apparatus claims, themselves show how to use the claimed invention, and (b) how to use the claimed invention was clear in the application as filed. Moreover, the Office Action, although incorrect in asserting that the claimed methods and apparatus are unpatentable, acknowledges that solving linear equations in the cryptographic art is standard. If uses for the solution to a set of linear equations in cryptography is known, such uses are still known even if a new and non-obvious method is used to obtain the solution. As such, Applicant respectfully requests that the 35 U.S.C. §112 rejection of claims 1-2, 4-26, and 28-32 be withdrawn.

Claims 1 and 25 were rejected under 35 U.S.C. §103(a) as being unpatentable over Curtis. In doing so, the Office Action asserts that Curtis teaches transforming a coefficient matrix into an upper triangular matrix using elementary row operations, and not division on the finite field GF(p). The Applicant respectfully traverses as the described transformation using elementary row operations does in fact include division on the finite field GF(p). This can be seen in the example of figure 95 where the matrixes A and I are subjected to elementary row operations that reduce A to the identity matrix.

In regard to the matrix A, to get from $\begin{bmatrix} 2 & -1 \\ 0 & \frac{3}{2} \end{bmatrix}$ to $\begin{bmatrix} 1 & -\frac{1}{2} \\ 0 & 1 \end{bmatrix}$, the elements of the top row

are divided by two, and the elements of the bottom row are both multiplied by two and divided

by three. The same holds true for changing the matrix I from $\begin{bmatrix} 1 & 0 \\ -\frac{3}{2} & 1 \end{bmatrix}$ to $\begin{bmatrix} \frac{1}{2} & 1 \\ -1 & \frac{2}{3} \end{bmatrix}$. As such,

the elements of each row are divided by the value of a diagonal element of that row in order to change the values of all the diagonal elements to 1. As such, Curtis includes division and thus does not satisfy the recitations of claim 1, claim 25, or any claim dependent on claims 1 or 25.

It should also be noted that the Office Action points to page 98, exercise 3 of Curtis to satisfy the recitation "solving the system of linear equations $Cx=d$ using the generated coefficient matrix C , the generated constant vector d , and the calculated inverses of the diagonal elements of the generated coefficient matrix C , to thereby solve the system of linear equations $Ax=bi$ of the read coefficient matrix A and the read constant vector b" However, exercise 3 is simply an exercise simply provides different matrixes A and B for use in solving the equation $Ax=B$. As such, there is no description as to how to solve the matrix equation, so there is no teaching or suggestion in the cited portion of Curtis to solve the equations in the manner claimed, i.e. using a generated coefficient matrix C , and calculated inverses of the diagonal elements of the generated coefficient matrix C . As such, the Applicant requests that the rejection of claims 1 and 25 be withdrawn.

Appl. No. 09/603,636
Amdt. dated April 4, 2005
Reply to Office action of January 5, 2005

Docket No. NAK1-BL53 (62478-1300)

Claims 2-24, and 26-32 were not rejected over the prior art. For the reasons provided above, the §101 and §112 rejections of those claims should be withdrawn, and the claims should be allowed.

It is believed that the case is now in condition for allowance, and an early notification of the same is requested. If the Examiner believes that a telephone interview will help further the prosecution of this case, he is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 4, 2005.


By: Rachel Carter

Rachel Carter
Signature

Dated: April 4, 2005

Very truly yours,

SNELL & WILMER L.L.P.



David J. Zoetewey
Registration No. 45,258
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4904